العنوان:	جرائم اختراق البيئة المعلوماتية وإستشراف الاتجاهات الحديثة في مجال أمن المعلومات : دراسة إبستيمولوجية في ضوء أراء عينة من المتخصصين
المصدر:	المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية- ICACC - كلية علوم الحاسب والمعلومات - جامعة الإمام محمد بن سعود الإسلامية - السعودية
المؤلف الرئيسي:	نوفل، هالة كمال احمد
مؤلفين آخرين:	إسماعيل، محمود حسن(م. مشارك)
محكمة:	نعم
التاريخ الميلادي:	2015
مكان انعقاد المؤتمر:	المملكة العربية السعودية. الرياض
رقم المؤتمر:	1
الهيئة المسؤولة:	جامعة الإمام محمد بن سعود الإسلامية. كلية علوم الحاسب والمعلومات
الشهر:	نوفمبر
الصفحات:	9 - 20
رقم MD:	690574
نوع المحتوى:	بحوث المؤتمرات
قواعد المعلومات:	HumanIndex
مواضيع:	أمن المعلومات
رابط:	http://search.mandumah.com/Record/690574

جرائم اختراق البيئة المعلوماتية واستشراف الاتجاهات الحديثة في مجال أمن المعلومات

دراسة إبستيمولوجية في ضوء أراء عينة من المتخصصين

أ. د/ هالة كمال أحمد نوفل

وكيل كلية الإعلام وتكنولوجيا الاتصال

جامعة جنوب الوادي

محافظة قنا، مصر

ص.ب: 83523 – جامعة جنوب الوادي – قنا –

ج.م.ع – الكيلو 6 طريق قنا – سفاجا

halaknofel@yahoo.com

أ.د/ محمود حسن إسماعيل

رئيس قسم الإعلام، معهد دراسات الطفولة

جامعة عين شمس

معهد دراسات الطفولة

جامعة عين شمس

القاهرة – مصر

Dr_mahmoud9@msn.com

الملخص – تثير جرائم اختراق البيئة المعلوماتية في المجتمعات الافتراضية العديد من الإشكاليات المتعلقة بالتنظيم القانوني، وآلياته، ومدى فعاليته، الأمر الذي يؤكد أهمية استطلاع رأي الخبراء والمتخصصين ممن لهم صلة بالقضية تجاه مجموعة من المتغيرات تدور حول طبيعة جرائم اختراق البيئة المعلوماتية لأنظمة المعلومات الإلكترونية على شبكة الإنترنت – الإشكاليات والحلول، وطرائق وضوابط الأمن المعلوماتي لغرض الحماية المعلوماتية اللازمة لمن يتعاملون مع الإنترنت واستشراف الاتجاهات المستقبلية الحديثة في مجال أمن المعلومات.

تعد هذه الدراسة من الدراسات الوصفية التشخيصية ذات المنحى التفسيري، وتعتمد على منهج المسح واستخدام أسلوب العينة العمدية والتي بلغ قوامها 240 مفردة، وطبقت في ثلاث محافظات هي: القاهرة وقنا والإسكندرية وكذلك في ست جامعات مصرية تمثل أنماطا مختلفة للتعليم في مصر وهي: جامعة جنوب الوادي والقاهرة، جامعة الأزهر، كليتي الفنية العسكرية والشركة، جامعتي 6 أكتوبر وجامعة مصر للعلوم والتكنولوجيا وأكاديمية أخبار اليوم، الجامعة الأمريكية في مصر.

أوضحت النتائج ارتفاع المتوسطات الحسابية بالنسبة لفئات المتخصصين والرأي في أنظمة الحماية الأمنية للمعلومات التي يجب أن تزودنا بها المواقع الإلكترونية على شبكة الإنترنت.

أشارت النتائج إلى ارتفاع المتوسطات الحسابية لمتغيرات انتقال المفتاح، والتحقق أحادي الجانب، والاعتراض والاحتيال، ومجال التشفير المحدود، والهجمات النشطة، وسلامة البيانات، في مقابل المحطة الطرفية وقلة الرؤية واختطاف القناة في ترتيب متأخر.

ثبتت صحة الغرض القائل بوجود علاقات إحصائية دالة بين فئات المتخصصين والرأي في المشكلات الموجودة في العناصر الأمنية المتاحة لآليات الحماية للمعلومات جزئيا.

حظيت جميع عناصر مظاهر الاعتداءات المختلفة على مواقع الإنترنت التي وردت بالاستمارة باهتمام فئات المتخصصين عينة الدراسة على اختلاف أنماط دراستها وهي: المسح، والنسخ غير المصرح به، وجمع والتقاط كلمات المرور، إنكار أو إلغاء الخدمة، السرقة أو الاختلاس، والتفتيش في مختلف التقنية، والعبث في البيانات، وهجمات المعطيات.

أوصت الدراسة بأهمية وجود رقابة على المواقع الإلكترونية بصورة لا تتقاطع مع الحرية للحد من استخدامها لأغراض سلبية ويكون ذلك عن طريق سن قوانين الجرائم المعلوماتية وإعداد برامج تهدف لدخول المجتمع المعلوماتي تنتهجها الدول.

الكلمات المفتاحية – اختراق المعلومات؛ جرائم الإنترنت؛ الأمن المعلوماتي؛ الحماية الأمنية؛ الرقابة على الإنترنت؛ الأنظمة الإلكترونية.

1. مقدمة

في إطار التحدي الجديد الذي تفرضه طبيعة الإنترنت كوسيط اتصالي وإعلامي بديل لانتشار الحريات، أصبحت ظاهرة جرائم اختراق المعلومات تشكل مصدر قلق وتهديد للأنظمة الإعلامية سواء السلطوية أو الليبرالية، كما سارعت هذه الأنظمة في التدخل

السريع لتنظيم وتجريم الاختراقات الأمنية لأنظمة الإنترنت، تارة بدعوى حماية الأطفال من المحتوى المعلوماتي الضار وغير الشرعي، وتارة ثانية بدعوى حماية الأمن القومي، وتارة ثالثة بزعم مكافحة العنصرية، فأرتفع عدد الدول التي تمارس رقابة كاملة على الإنترنت إلى أكثر من 80 دولة [1]، بينما منعت الحكومة الأمريكة الآلاف من أجهزة التشفير خوفا من استخدامها من قبل منظمات إرهابية، كما كثفت وكالة المخابرات الأمريكية المركزية جهودها لتعقب نشاطات بعض المنظمات التي تدعى العمل في مجال الدفاع عن حريات التعبير بالتعاون مع مكتب التحقيقات الفيدرالية[2]، الأمر الذي يعكس إزدوجيات المعايير؛ حيث تواجه الأولى استراتيجيات الرقابة خارج حدودها، وتواجه الثانية تبني استراتيجيات أكثر صرامة وتقدما داخل حدودها[3].

هكذا تثير جرائم اختراق البيئة المعلوماتية في المجتمعات الافتراضية العديد من الإشكاليات المتعلقة بالتنظيم القانوني، وآلياته، ومدى فعاليته، الأمر الذي يؤكد أهمية استطلاع رأي الخبراء والمتخصصين ممن لهم صلة بالقضية من الإعلاميين والأكاديميين والتربويين والعسكريين والقضائيين، ومهندسي نظم المعلومات والاتصالات والكمبيوتر، تجاه مجموعة من المتغيرات تدور حول طبيعة جرائم اختراق البيئة المعلوماتية لأنظمة المعلومات الإلكترونية على شبكة الإنترنت – الإشكاليات والحلول، وطرائق وضوابط الأمن المعلوماتي لغرض الحماية المعلوماتية اللازمة لمن يتعاملون مع الإنترنت واستشراف الاتجاهات المستقبلية الحديثة في مجال أمن المعلومات[4].

2. مشكلة الدراسة

مع بروز مناطق جديدة للصراع في العالم وتغير الطبيعة المعلوماتية للأنظمة والدول، أصبح الاختراق من أجل الحصول على المعلومات مسألة بالغة الأهمية والخطورة، حيث أدت ثورة المعلومات إلى انتشار لصوص الحاسب الآلي وجرائم الإنترنت الحديثة[5]، كما أن الجانب المظلم للمعلومات هو استثمارها في جوانب مهددة للأمن البشري، وكأداة في الهجوم المعلوماتي على الخصم، أو كمصدر من مصادر التهديد الأمني لأنها تمثل رابطا تعتمد عليها العديد من القطاعات مما يسهل الإضرار بمصالح الطرف المقابل أو الاستفادة منه دون عناء أو كلاهما[6].

وبالتالي فإن هذه الدراسة تسعى لاستطلاع رأي الجمهور المتخصص والمثقف حول جرائم اختراق البيئة المعلوماتية في المجتمعات الافتراضية وإشكالياتها وسبل حماية نظم الأمن المعلوماتية، وعناصرها، وكيفية وإمكانية تفعيل دورها من وجهة نظرهم، وكذلك التعرف على رأيهم ووجهات نظرهم حول ماهية وطبيعة البيانات والمعلومات المراد حمايتها، والمخاطر التي تتطلبها هذه الحماية، وكيفية توفير تلك الحماية، وماهية العمليات الرئيسية المتصلة بأمن المعلومات، وطبيعة رسائل التوثيق من المستخدمين وحدود وصلاحيات الاستخدام فيها.

3. أهمية الدراسة:

ترجع أهمية الدراسة لما يلي:

- حداثة الموضوع وأهميته وانتشاره في الوقت الحالي. وعدم المعرفة أو الإلمام الكافي والواعي بالقوانين وأنظمة الحماية والتأمين لتكنولوجيا الأمن المعلوماتي ولكثير من برمجيات الحواسيب وتقنياتها التكنولوجية. والاختراعات الجديدة والمستحدثة على شبكة الويب. ورغبة البعض وقدرته أحيانا على التعدي على خصوصيات الآخرين لاختراقها أو سرقتها أو إتلافها وتدميرها وما إلى ذلك من الجرائم المعلوماتية.

4. الهدف العام للدراسة:

تسعى الدراسة لاستطلاع آراء عينة من الجمهور المتخصص متمثل في أساتذة الجامعات المهتمين بشئون الإعلام والحاسبات والمعلومات، وكذلك المتخصصون في القانون والهندسة والتربية ورجال الدين والقضاء والعسكريون حول طبيعة وإشكاليات جرائم اختراق البيئة المعلوماتية في المجتمعات الافتراضية، وكيفية التصدي لهذه الظاهرة في ضوء نظرية التماس المعلومات ونظرية الابستمولوجية والتي تعني بعلم المفاهيم ودراسته في الفكر الابستمولوجي الفلسفي [7] والتي تتبنى الباحثة منطلقاتها في هذه الدراسة للسعي وراء تعريف وتفسير ووصف وفهم طبيعة المفاهيم العلمية والتكنولوجية الحديثة التي تسوقها لنا هذه الدراسة في مجال تكنولوجيا الأمن المعلوماتي والمتعلقة بجرائم اختراق البيئة المعلوماتية والإنترنت واستشراف الاتجاهات الحديثة في مجال أمن المعلومات في المرحلة الأولى، ثم قياس

علاقة هذه التعريفات والمفاهيم وربطها بآراء عينة من المتخصصين ذوي العلاقة المباشرة في التعامل مع طبيعة هذه المعلومات في سعيهم لالتماس المعلومات في المجتمعات الافتراضية في المرحلة الثانية.

5. نوع الدراسة ومنهجها:

تعد هذه الدراسة من الدراسات الوصفية التشخيصية ذات المنحى التفسيري التي تهدف إلى تحليل وتشخيص وتقييم خصائص ظاهرة جرائم اختراقات البيئة المعلوماتية في المجتمعات الافتراضية على شبكة الإنترنت، ووسائل وسبل الحماية والتدابير التي يجب اتخاذها لمعالجة القضية المطروحة، سعيا لإيجاد رؤية استراتيجية فعالة لحماية المعلومات.

وتعتمد الدراسة على منهج المسح لجمهور وسائل الإعلام بما يمكن من الحصول على البيانات الست من المبحوثين وهي: (الحقائق؛ الإدراك؛ الآراء؛ الاتجاهات؛ المعرفة؛ والخصائص الديموغرافية) [8]

6. أدوات جمع البيانات

اعتمدت الدراسة على استمارة الاستبيان التي احتوت على أسئلة مفتوحة وأخرى مغلقة للاستفادة من كلا النوعين، كما احتوت على مقاييس تجميعية مختلفة وكذلك الاعتماد على مقياس ليكرت لقياس بعض اتجاهات المبحوثين حول الظاهرة المدروسة، وقد تم تصميمها في إطار منهج المسح بأسلوب المقابلة المقننة.

7. عينة الدراسة وحجمها

تم استخدام أسلوب العينة العمدية لعدم توافر أطر وخصائص مشتركة تجمع فئات الجمهور المتخصص لهذا البحث ليتم سحب عينة منها، ولذلك تم سحب العينة بطريقة عمدية Purposive Sample وهي من العينات غير الاحتمالية Non-Probability Sample [9]، وحتى تتمكن من توفير بعض السمات الخاصة والخصائص المشتركة في أفراد العينة وتجمع بين فئات الجمهور المتخصص الخمس حيث اقتصرت على من يتعاملون مع أجهزة الكمبيوتر سواء بحكم عملهم أو تخصصاتهم أو دراستهم، كذلك لديهم خبرة ومعرفة ببرامج الحماية الأمنية المختلفة لأجهزة للكمبيوتر سواء في مجال السوفت (Software) أو الهارد وير (Hardware)، وقد بلغ حجم العينة 240 مفردة، كما طبقت هذه الدراسة في ثلاث محافظات هي:

القاهرة وقنا والإسكندرية، وفي ست جامعات في مصر تمثل أنماطا مختلفة للتعليم في مصر وهي [10]:

1- جامعة جنوب الوادي والقاهرة كمثال لنمط التعليم العام (المدني العلماني) في مصر.

2- جامعة الأزهر في القاهرة والأقصر كمثال لنمط التعليم الأزهري والديني في مصر.

3- كليتي الفنية العسكرية والشرطة وتمثلان نمطي التعليم العسكري في مصر.

4- جامعتي 6 أكتوبر وجامعة مصر للعلوم والتكنولوجيا وأكاديمية أخبار اليوم كنماذج لنمط التعليم الخاص (الاستثماري والربحي) متمثل في كليتي (الهندسة والاتصالات – الإعلام).

5- الجامعة الأمريكية في مصر كنموذج لنمط التعليم الأجنبي في مصر متمثل في كليتي (الإعلام والهندسة) ومركز المعلومات وصيانة معامل الكمبيوتر بالجامعة.

8. مقاييس الدراسة

قاما الباحثان بحصر مقاييس الدراسة والتي بلغت ستة مقاييس تجميعية اشتملت بنودها على 61 بندا كالتالي:

فأشتمل المقياس الأول على 25 بندا والثاني على سبع مقاييس، والثالث على سبعة مقاييس والرابع على عشرة بنود والخامس على ثمانية بنود، والسادس على أربعة بنود، وتم تقسيمها إلى مجموعة من المقاييس الرئيسية والفرعية التي تجيب على فروض الدراسة كالآتي:

1- مقياس خرق الحماية الأمنية المتصلة بالمعطيات والمتعلقة بأشخاص [11] ويشمل:

التفتيش في مخلفات التقنية – الالتقاط اللاسلكي – استراق الأمواج – إنكار أو إلغاء الخدمة – التخفي بانتحال شخص مفوض.

الهندسة الاجتماعية – الإزعاج والتحرش – قرصنة البرمجيات – هجمات المعطيات – النسخ غير المصرح به – تحليل الاتصالات – القنوات المخفية – هجمات البرمجيات – المصائد أو الأبواب الخلفية – السرقة أو اختلاس المعلومة أو الاستخدام اللحظي – الهجمات عبر التلاعب بنقل المعطيات عبر أنفاق النقل – الهجمات الوقتية – المعطيات الاعتيادية.

البرمجيات الخبيثة – العبث والغش بالبيانات – خداع بروتوكول الإنترنت – جمع والتقاط كلمات المرور – المسح والنسخ.

هجمات استغلال المزايا الإضافية –كل ما سبق.

2- أهم أشكال الحماية الأمنية المتاحة على شبكة الإنترنت [12] ويشمل:

استخدام كلمات السر – استخدام برامج مقاومة للفيروسات – برامج حماية الدخول لشبكة الإنترنت – الجدران النارية.

تشفير البيانات – وضع سياسة لأمن المعلومات خاصة بكل مؤسسة –كل ما سبق.

3- العناصر الأمنية المفضل وجودها على شبكة الإنترنت [13] وتشمل:

التوثيق – التشفير – السرية – وحدة هوية المشترك – طبقة التطبيقات الأمنية – الشفافية – الثقة.

4- مشكلات آليات الحماية الأمنية للمعلومات وتشمل [14]:

اختطاف القناة – سلامة البيانات – التحقق الأحادي الجانب – خوارزميات التشفير الضعيف – المحطة الطرفية غير الآمنة.

الاعتراض والاحتيال القانوني – قلة الرؤية أو الوضوح – الهجمات النشطة – انتقال المفتاح – مجال التشفير المحدود.

5- أوجه التحديات التي تواجه تكنولوجيا الأمن المعلوماتي وتشمل:

أ- تحديات على المستوى العالمي: تحديات سياسية – اقتصادية – تكنولوجية وفنية – أمنية.

ب- تحديات داخلية: التنمية والديموقراطية وحقوق الإنسان – التحديات البشرية ونقص الكفاءات – التحديات الثقافية.

التحديات التربوية – التحديات الأمنية.

6- أشكال التهديدات التي تواجه اختراق البيئة المعلوماتية [15] وتشمل:

التهديد بالاضطراب في أنظمة الاتصالات – التهديد باستغلال المعلومات – التهديد بالتلاعب في البيانات – التهديد بتدمير البيانات.

9. فروض الدراسة

أولا: توجد علاقة ارتباطية دالة إحصائيا بين المتغيرات الديموغرافية لعينة الدراسة (فئات المتخصصين – نمط التعليم) وكل من المتغيرات المدروسة على النحو التالي:

1- توجد علاقة ارتباطية دالة إحصائيا بين المتغيرات الديموغرافية لعينة الدراسة (فئات المتخصصين – نمط التعليم) والرأي في مظاهر الاعتداءات المختلفة على مواقع الإنترنت.

2- توجد علاقة ارتباطية دالة إحصائيا بين المتغيرات الديموغرافية لعينة الدراسة (فئات المتخصصين – نمط التعليم) والرأي في العناصر الأمنية المفضل وجودها داخل أجهزة الكمبيوتر ومواقع الإنترنت كحماية لأمن المعلومات من وجهة نظرهم.

3- توجد علاقة ارتباطية دالة إحصائيا بين المتغيرات الديموغرافية لعينة الدراسة (فئات المتخصصين – نمط التعليم) والرأي في أشكال الحماية التي يجب توافرها على شبكة الإنترنت.

4- توجد علاقة ارتباطية دالة إحصائيا بين المتغيرات الديموغرافية لعينة المتخصصين (فئات المتخصصين – نمط التعليم) والرأي في المشكلات الموجودة في العناصر الأمنية المتاحة.

5- توجد علاقة ارتباطية دالة إحصائيا بين المتغيرات الديموغرافية لعينة الدراسة (فئات المتخصصين – نمط التعليم) والرأي في التحديات التي تواجه أنظمة وعناصر الحماية الأمنية للمعلومات.

6- توجد علاقة ارتباطية دالة إحصائيا بين المتغيرات الديموغرافية لعينة الدراسة (فئات المتخصصين – نمط التعليم) والمهددات الأمنية لأنظمة المعلومات المتاحة من وجهة نظرهم.

7- توجد علاقة ارتباطية دالة إحصائيا بين المتغيرات الديموغرافية لعينة الدراسة (فئات المتخصصين – نمط التعليم) وأنظمة الحماية الأمنية للمعلومات.

ثانيا: توجد علاقة ارتباطية دالة إحصائيا بين كثافة تعرض المبحوثين للإنترنت وكلا من:

مستوى التزود بالمعلومات الأمنية. مستوى خرق الحماية المادية. مستوى خرق الحماية المتعلقة بالأشخاص وشئون الموظفين. مستوى خرق الحماية المتصلة بالاتصالات والمعطيات. مستوى التحديات العالمية. مستوى التحديات الداخلية.

نتائج الدراسة الميدانية واختبار صحة الفروض

1- تبين ارتفاع المتوسطات الحسابية بالنسبة لفئات المتخصصين عينة الدراسة والرأي في أنظمة الحماية الأمنية للمعلومات التي يجب أن تزودنا بها المواقع الإلكترونية على شبكة الإنترنت وهي: تحديات تواجه شبكات المعلومات في الترتيب الأول يليه أنظمة حماية أمنية خاصة للمعلومات في الترتيب الثاني، ثم تحليل أنظمة الاتصالات في الترتيب الثالث، ثم أنظمة التشفير ومجالاتها، فالقنوات المخفية في الترتيب الرابع والخامس، كذلك برامج مقاومة الفيروسات في الترتيب السادس فقرصنة البرمجيات وكيفية استراق الأمواج في الترتيب السابع والثامن ثم أنظمة اختراق مجال المعلومات والأنظمة الأمنية في الترتيب التاسع فالنسخ غير المصرح به في الترتيب قبل الأخير ثم كيفية الاستغلال المسموح وغير المسموح به للمعلومات في الترتيب الأخير.

يتضح من جداول التحليل وجود فروق جوهرية في متغير أنظمة الحماية الأمنية الخاصة في مجال المعلومات وذلك عند مستوى دلالة (0.003) وكذلك في متغير استراق الأمواج بمستوى دلالة (0.023) وقرصنة البرمجيات بمستوى دلالة (0.029) والنسخ غير المصرح به بمستوى دلالة (0.049) وتحليل الاتصالات بمستوى دلالة (0.004)، وبذلك ثبت وجود علاقة إحصائية دالة في خمسة متغيرات فقط من أصل إحدى عشر متغيرا بالنسبة للعلاقة بين فئات المتخصصين عينة الدراسة. والرأي في وجود أنظمة حماية مختلفة في مواقع الإنترنت، وبالتالي ثبت صحة هذا الفرض جزئيا في المتغير الأول والسابع والثامن والتاسع والعاشر، بينما لم يثبت صحته بالنسبة لباقي المتغيرات المدروسة.

ارتفاع المتوسطات لكل من عينة الأكاديميين والمحامين ورجال القضاء والدين على التوالي في مقابل انخفاض تلك المتوسطات لدى فئتي المتخصصين العسكريين والأكاديميين على التوالي وذلك بالنسبة لمتغيرات تشفير البيانات ووضع سياسة لأمن المعلومات خاصة بكل مؤسسة وكل ما سبق.

أفادت النتائج بالنسبة للمتوسطات الحسابية الإجمالية لمتغير أشكال الحماية التي يجب توافرها بصفة عامة على شبكة الإنترنت كانت في الترتيب الأول متغير برامج حماية الدخول على شبكة الإنترنت والجدران النارية في الترتيب الثاني واستخدام كلمة السر في الترتيب الثالث ووضع سياسة لأمن المعلومات في الترتيب الرابع، في مقابل كل ما سبق في الترتيب الخامس واستخدام برامج مقاومة للفيروسات في الترتيب السادس وتشفير البيانات في الترتيب السابع والأخير.

كما ثبت جزئيا صحة الفرض القائل بوجود علاقة دالة إحصائيا بالنسبة لثلاث متغيرات فقط وهي؛ استخدام برامج مقاومة للفيروسات، وبرامج حماية الدخول للشبكة، وكل ما سبق، وذلك بمستوى دلالة = (0.049) و(0.043) و(0.005) على التوالي، بينما لم تثبت صحته بالنسبة لبقية المتغيرات المدروسة.

أشارت النتائج إلى ارتفاع المتوسطات الحسابية الإجمالية لمتغيرات انتقال المفتاح في الترتيب الأول، والتحقق أحادي الجانب في الترتيب الثاني، والاعتراض والاحتيال في الترتيب الثالث، ومجال التشفير المحدود والهجمات النشطة في الترتيب الرابع والرابع مكرر، وسلامة البيانات في الخامس، في مقابل المحطة الطرفية في ترتيب متأخر نسبيا وهو السادس، ثم قلة الرؤية في الترتيب قبل الأخير فاختطاف القناة في الترتيب الأخير. ويرجع الباحثان عدم استطاعة عينة الدراسة التفريق بين مختلف المشكلات الموجودة في العناصر الأمنية لأليات حماية المعلومات إلى حداثة الموضوع. واختلاف فئات العينة المدروسة ووظائفها وتخصصاتها، وإلى الفروق الملحوظة في المتوسطات الحسابية. وكذلك اختلاف أماكن سحب العينة.

ثبتت صحة الفرض والقائل بوجود علاقات إحصائية دالة بين فئات المتخصصين والرأي في المشكلات الموجودة في العناصر الأمنية المتاحة لآليات الحماية للمعلومات جزئيا، حيث تبين وجود علاقات في ثلاثة متغيرات فقط من أصل عشرة متغيرات في هذا

المقياس وهي: التحقق أحادي الجانب، والمحطة الطرفية الآمنة، وقلة الرؤية والوضوح، بينما لم يثبت صحته بالنسبة لباقي المتغيرات المدروسة.

أشارت النتائج الإجمالية لقيمة المتوسطات الحسابية ارتفاع مؤشرات متغيرات التهديد بتدمير البيانات في الترتيب الأول، ثم التهديد باستغلال المعلومات في الترتيب الثاني، ثم الإبقاء على المعلومات في الترتيب الثالث، وأخيرا التهديد بالاضطراب في أنظمة الاتصالات في الترتيب الرابع والأخير. ويبدو أن متغير التهديد بتدمير البيانات هو الأكثر شيوعا واستخداما لدى أفراد المتخصصين عينة الدراسة حيث أشاروا إليه في الترتيب الأول على أنه الأكثر خطورة وأهمية على الإطلاق من وجهة نظرهم.

وثبت وجود علاقة دالة إحصائيا بين جميع العناصر المدروسة لهذا المقياس مع فئات المتخصصين عينة الدراسة، وبالتالي ثبت صحة هذا الفرض القائل بوجود علاقة بين فئات المتخصصين وأهم المهددات الأمنية لأنظمة المعلومات من وجهة نظرهم.

أظهرت النتائج تفوق إجابات أفراد عينة الدراسة بالنسبة لذوي جميع أنماط التعليم بنسب متفاوتة بالنسبة لوضع برامج مقاومة للفيروسات، وكذلك التأمين ضد النسخ غير المصرح به للمعلومات، بينما ذكرت عينتي ذوي نمط التعليم المدني والأزهري جميع متغيرات أنظمة الحماية بنسب متفاوتة، في حين لم يذكر أفراد عينة ذوي نمط التعليم الخاص سوى سبع متغيرات فقط من جملة إحدى عشر متغيرا، وبالنسبة لذوي نمط التعليم الأجنبي ستة متغيرات فقط من جملة إحدى عشر متغيرا، وذوي نمط التعليم العسكري سبع متغيرات من أصل إحدى عشر متغيرا ولكن بفروق طفيفة، مما يشير إلى تقارب وجهات النظر بالنسبة للرأي في أنظمة الحماية الأمنية التي يجب أن تتبع في مجال أمن المعلومات وأنماط التعليم المختلفة المدروسة لأصحاب العينة.

وجود شبه إجماع من المبحوثين على أن جميع عناصر مظاهر الاعتداءات المختلفة على مواقع الإنترنت التي وردت بالاستمارة مهمة وحظيت باهتمام فئات المتخصصين عينة الدراسة على اختلاف أنماط دراستها، بينما أشار بعض المبحوثين لبعض عناصر البدائل المختلفة تبعا لأهميتها بالنسبة لهم نذكر منها كما يوضح الجدول السابق: المسح، والنسخ، والنسخ غير المصرح به، وجمع والتقاط كلمات المرور، وإنكار أو إلغاء الخدمة، والسرقة أو الاختلاس، والتفتيش في مخلفات التقنية، والعبث في البيانات، وهجمات المعطيات.

على مستوى البيانات التفصيلية يتضح اهتمام وترشيح أصحاب عينة ذوي نمط التعليم المدني والأزهري لجميع عناصر وأشكال ومظاهر الاعتداءات على مواقع الإنترنت المختلفة من وجهة نظرهم، بينما اهتمت عينة نمط التعليم الخاص بمعظمها، أما عينة نمط التعليم الأجنبي فقد أشارت إلى التفتيش في مخلفات التقنية، والإزعاج والتحرش، وقرصنة البرمجيات، وهجمات المعطيات والمصائد أو الأبواب الخلفية، وجمع والتقاط كلمات المرور كمظاهر هامة للاعتداء على مواقع الإنترنت من وجهة نظرهم، بينما اهتمت عينة أصحاب نمط التعليم العسكري بموضوعات القرصنة والهجمات النشطة، كالمعطيات والبرمجيات الوقتية والاعتيادية، والخدع، وجمع والتقاط كلمات المرور، والمسح، والنسخ، ويبدو أن هذه المظاهر تدخل ضمن برنامج أو مقرر تدريبي أو عملي يرتبط بنطاق تخصصاتهم أو وظائفهم أو دراستهم العسكرية وبالتالي أنعكس على ترشيحاتهم لمظاهر الاعتداءات المختلفة على مواقع الإنترنت التي وردت في إجاباتهم من وجهة نظرهم.

وبصفة عامة أظهرت الاختبارات الإحصائية وجود علاقات ارتباطية دالة إحصائيا بين ستة عشر متغيرا من أصل 25 متغيرا مدروسا للعلاقة بين مظاهر الاعتداءات على مواقع الإنترنت ونمط التعليم، وذلك عند مستوى دلالة (0.05) مما يثبت صحة هذا الفرض جزئياً.

يتضح تفوق أفراد عينة الدراسة من ذوي نمط التعليم العام والعسكري في ضرورة استخدام برامج حماية عند الدخول لشبكة الإنترنت في الترتيب الأول، ثم الجدران النارية، فوضع سياسة لأمن المعلومات في الترتيب الثاني وذلك من وجهة نظر ذوي نمط التعليم العسكري والخاص، بينما أتت بقية أشكال التعليم بنسب متفاوتة بعد ذلك في ترتيب متأخر نسبياً. وثبت وجود علاقات إحصائية دالة في المتغير الأول والثاني والثالث والخاص باستخدام كلمة السر واستخدام برامج مقاومة للفيروسات وبرامج حماية الدخول لشبكة الإنترنت وكذلك في المتغير السادس والسابع والمتعلق بوضع سياسة لأمن المعلومات الخاصة بكل مؤسسة وكل ما سبق، بينما لم يثبت وجود هذه العلاقات بالنسبة لمتغيرين فقط وهما الجدران النارية، وتشفير البيانات، مما يثبت صحة هذا الفرض القائل بوجود علاقات إحصائية دالة بين نمط التعليم وأشكال الحماية المطلوب توافرها على شبكة الإنترنت.

يتضح اهتمام وترشيح أصحاب عينة ذوي نمط التعليم المدني والأزهري لجميع عناصر وأشكال ومظاهر الاعتداءات على مواقع الإنترنت المختلفة من وجهة نظرهم، بينما اهتمت عينة نمط التعليم الخاص بمعظمها، أما عينة نمط التعليم الأجنبي فقد أشارت إلى التفتيش في مخلفات التقنية، والإزعاج والتحرش، وقرصنة البرمجيات، وهجمات المعطيات والمصائد أو الأبواب الخلفية، وجمع والتقاط كلمات المرور كمظاهر هامة للاعتداء على مواقع الإنترنت من وجهة نظرهم.

اهتمت عينة أصحاب نمط التعليم العسكري بموضوعات القرصنة والهجمات النشطة، كالمعطيات والبرمجيات الوقتية والاعتيادية، والخدع، وجمع والتقاط كلمات المرور، والمسح، والنسخ، ويبدو أن هذه المظاهر تدخل ضمن برنامج أو مقرر تدريبي أو عملي يرتبط بنطاق تخصصاتهم أو وظائفهم أو دراستهم العسكرية وبالتالي أنعكس على ترشيحاتهم لمظاهر الاعتداءات المختلفة على مواقع الإنترنت التي وردت في إجاباتهم من وجهة نظرهم.

بصفة عامة أظهرت النتائج وجود علاقات ارتباطية دالة إحصائياً بين ستة عشر متغيراً من أصل 25 متغيراً مدروساً وهي: التفتيش في مخلفات التقنية واستراق الأمواج وإنكار أو إلغاء الخدمة وهجمات المعطيات والنسخ غير المصرح به والقنوات المخفية والسرقة أو اختلاس المعلومة والهجمات الوقتية والعمليات الاعتيادية والبرمجيات الخبيثة والعبث والغش في البيانات وخداع بروتوكول الإنترنت وجمع والتقاط كلمات المرور والمسح والنسخ وهجومات استغلال المزايا الإضافية وكل ما سبق. للعلاقة بين مظاهر الاعتداءات على مواقع الإنترنت ونمط التعليم، وذلك عند مستوى دلالة (0.05) مما يثبت صحة هذا الفرض جزئيا.

أوضحت البيانات التفصيلية تفوق أفراد عينة الدراسة من ذوي نمط التعليم العام بالنسبة لعنصر التوثيق، ثم التشفير ووحدة هوية المشترك في الترتيب الثاني والثاني مكرر، بينما تراجعت بقية المتغيرات إلى ترتيبات متأخرة نسبيا، بينما في التعليم الأزهري أوضحت النتائج تفوق إجابات المبحوثين بالنسبة لعنصر الشفافية والتوثيق والسرية، وفي نمط التعليم الخاص والأجنبي تفوقت إجابات المبحوثين بالنسبة لعنصر التشفير، في حين تفوقت إجابات المبحوثين في نمط التعليم الخاص بالنسبة لعنصر وحدة هوية المشترك، وربما يعود هذا الاختلاف في إجابات المبحوثين إلى عدم قدرة بعضهم على تحديد بعض هذه العناصر الأمنية المفضل وجودها داخل أجهزة الكمبيوتر والإنترنت على وجه الدقة، علما بأنه تم إرفاق التعريفات الإجرائية مع استمارة الاستقصاء.

ثبت وجود علاقات إحصائية دالة بالنسبة لخمس متغيرات فقط من أصل سبع متغيرات وهي: استخدام كلمة السر واستخدام برامج مقاومة للفيروسات وبرامج حماية الدخول لشبكة الإنترنت ووضع سياسة لأمن المعلومات خاصة بكل مؤسسة وكل ما سبق، بينما لم يثبت وجودها في متغيرين فقط وهما: تشفير البيانات والجدران، مما يجعلنا نقبل جزئيا صحة الفرض القائل بوجود علاقات إحصائية دالة بين نمط التعليم وعناصر الحماية الأمنية المفضل وجودها في أجهزة الكمبيوتر.

توجد علاقة إحصائية دالة بين كثافة تعرض المبحوثين عينة الدراسة ومقياس التزود بالمعلومات الأمنية تفيد أن أن المبحوثين عينة الدراسة كثيفو التعرض للإنترنت لديهم معلومات عن برامج الحماية الأمنية المتاحة للكمبيوتر والإنترنت أكثر من المبحوثين متوسطي التعرض الذي جاء في الترتيب الثاني، وكذلك المبحوثين ضعيفو التعرض في الترتيب الثالث والأخير.

توجد علاقة دالة إحصائيا بين مقياس خرق الحماية المادية وتعرض المبحوثين للمعلومات الخاصة، بذلك تفيد أن المبحوثين كثيفو التعرض عينة الدراسة أكثر خبرة ودراية بهذا الموضوع عن غيرهم في الترتيب الأول، يليهم متوسطي التعرض في الترتيب الثاني، ثم ضعيفي التعرض في الترتيب الثالث والأخير وذلك عند مستوى معنوية (0.020).

18- توجد علاقة إحصائية دالة بين مقياس خرق الحماية المتعلقة بالأشخاص وشئون الموظفين وتعرض المبحوثين لهذا النوع من المعلومات تفيد أن المبحوثين كثيفو التعرض عينة الدراسة أكثر خبرة ودراية بهذا الموضوع في الترتيب الأول، يليهم متوسطي التعرض في الترتيب الثاني، ثم ضعيفي التعرض في الترتيب الثالث والأخير وذلك عند مستوى معنوية (0.007).

أشارت النتائج إلى أن المبحوثين كثيفو التعرض لبرامج خرق الحماية المتصلة بالاتصالات والمعطيات، وأنواع التحديات العالمية والداخلية التي تواجه أمن المعلومات على علم ودارية وخبرة بالمعلومات وكيفية التصرف إزاء ذلك، يليهم متوسطي التعرض في الترتيب الثاني، ثم ضعيفو التعرض في الترتيب الثالث والأخير، بينما لم تثبت وجود علاقات إحصائية دالة بينهم وبين هذه المتغيرات المدروسة، مما يجعلنا نقبل جزئيا الفرض القائل بوجود علاقة بين المقاييس التجميعية للمتغيرات المدروسة في البحث وبين كثافة تعرض المبحوثين لها

ولبرامجها وذلك بالنسبة لمقياس التزود بالمعلومات الأمنية، ومستوى خرق الحماية المادية، ومستوى خرق الحماية المتعلقة بالأشخاص وشئون الموظفين.

ارتفاع معدلات تعرض الذكور للموضوعات الاقتصادية والجريمة والحوادث والأخبار العلمية والتكنولوجية والجديد في مجال علوم الكمبيوتر والرياضة واكتشاف ما هو جديد وراء الإنترنت عن الإناث، في مقابل ارتفاع معدلات تعرض الإناث عينة الدراسة للموضوعات السياسية والاجتماعية والثقافية والعلمية والمتعلقة بالمرأة والترفيه وأخبار الاختراعات والإلكترونيات.

ثبت جزئيا صحة الفرض القائل بوجود علاقة بين النوع والرأي في التحديات التي تواجه أنظمة الحماية الأمنية للمعلومات بالنسبة لمتغيرات برامج مقاومة الفيروسات، وأنظمة اختراق مجال المعلومات، وكيفية الاستغلال المسموح أو غير المسموح للمعلومات، ومتغير النسخ غير المصرح به، وتحليل الاتصالات، والقنوات المخفية المدروسين.

ثبت جزئيا صحة الفرض القائل بوجود علاقة بين النوع وأنواع ومظاهر الاعتداءات المختلفة على مواقع الإنترنت المدروسة من وجهة نظر المتخصصين عينة الدراسة بالنسبة للمتغير المتعلق بمظاهر اختراق الحماية الأمنية المتصلة بالأشخاص وشئون الموظفين لصالح الذكور، كما ثبتت صحة هذا الفرض أيضا في وجود علاقات ارتباطية وإحصائية دالة في مجموعة خرق الحماية المتصلة بالاتصالات والمعطيات في المجموعة الثانية أغلبها لصالح الإناث.

ارتفاع رؤية المتخصصين من الذكور عينة الدراسة لأوجه التحديات العالمية التي تواجه تكنولوجيا الأمن المعلوماتي في المجموعة الأولى والخاصة بالتحديات العالمية الاقتصادية والفنية والتكنولوجية وفي المجموعة الثانية، بالنسبة لتحديات التنمية والديموقراطية وحقوق الإنسان والتحديات البشرية ونقص الكفاءات والتحديات الثقافية والتربوية، في مقابل ارتفاع مؤشرات رؤية الإناث عينة الدراسة لأوجه التحديات المختلفة التي تواجه تكنولوجيا المعلومات والأمن المعلوماتي بالنسبة للتحديات السياسية والأمنية، وقد ثبت صحة هذا الفرض بالنسبة لجميع المتغيرات المدروسة.

ثبتت صحة الفرض القائل بوجود علاقة بين النوع وأشكال التهديدات التي يواجهها الأمن المعلوماتي بالنسبة لجميع المتغيرات المدروسة، يفسرها أن الذكور على علم بأشكال التهديدات التي تواجه مجال الأمن المعلوماتي واختراق البيئة الافتراضية أكثر من الإناث.

ثبت صحة الفرض القائل بوجود علاقة بين التعرض للمواقع المختلفة عبر شبكة الإنترنت وفئات المتخصصين عينة الدراسة تفيد ارتفاع نسبة تعرض فئتي العسكريين والتربويين لمواقع البحوث العلمية والبرمجيات وتحليل النظم، في مقابل ارتفاع نسبة تعرض المهندسين بتخصصاتهم المختلفة للبريد الإلكتروني بفارق نسبي كبير، في حين أرتفع الإقبال على مواقع المدونات والمنتديات لدى فئات الأكاديميين ورجال القضاء والدين، وتساوت تقريبا في التعرض والإقبال لدى فئات المتخصصين بالنسبة لمواقع التواصل الاجتماعي والمواقع الإعلامية، وبفروق طفيفة في المتوسطات الحسابية.

ثبت صحة الفرض القائل بوجود علاقة بين فئات المتخصصين تفيد ارتفاع نسبة تعرض النخبة الأكاديمية والعسكرية والقضاة ورجال الدين طبقا لدوافع نفعية، بينما ترتفع نسبة تعرض التربويين للإنترنت بدوافع شبه نفعية، بينما قلت أو أنتفت تقريبا الدوافع الطقوسية لتعرض هذه الفئات للإنترنت كما تتفق هذه النتيجة مع نتائج دراستي "سميشي وداد" و"نور هادف" [16].

ثبت جزئيا وجود علاقة دالة إحصائيا بين فئات المتخصصين عينة الدراسة والرأي في أنظمة الحماية الأمنية للمعلومات التي يجب أن تزودنا بها المواقع الإلكترونية على شبكة الإنترنت وذلك بالنسبة لمتغيرات أنظمة الحماية الأمنية الخاصة بمجال المعلومات عند مستوى دلالة (0.003) وكذلك في متغير استراق الأمواج بمستوى دلالة (0.023) وقرصنة البرمجيات بمستوى دلالة (0.029) والنسخ غير المصرح به بمستوى دلالة (0.049) وتحليل الاتصالات بمستوى دلالة (0.004).

ثبت جزئيا وجود علاقة بين فئات المتخصصين عينة الدراسة وأشكال ومظاهر الاعتداءات واختراق البيئة المعلوماتية على الإنترنت بالنسبة لخمسة عشر متغيرات مدروسا من أصل خمس وعشرون متغيرا، وذلك عند مستوى دلالة (0.05) أو أقل.

ثبتت صحة هذا الفرض جزئيا والقائل بوجود علاقات إحصائية دالة بين فئات المتخصصين والرأي في المشكلات الموجودة في العناصر الأمنية المتاحة لآليات الحماية للمعلومات، حيث تبين وجود علاقات في ثلاثة متغيرات فقط من أصل عشرة متغيرات في هذا المقياس وهي: التحقق أحادي الجانب، والمحطة الطرفية الآمنة، وقلة الرؤية والوضوح.

ثبت صحة الفرض القائل بوجود علاقات إحصائية دالة بين نمط التعليم ونوعية الموضوعات التي يقبل عليها المتخصصون عينة الدراسة والتي تقع كلها في دائرة الاهتمامات النفعية، بينما أنتفت الدوافع الطقوسية، فثبت وجود علاقات إحصائية دالة بالنسبة للموضوعات السياسية، والاقتصادية، والاجتماعية، والعلمية، والرياضية، وأخبار الاختراعات، والجديد في مجال الكمبيوتر، واكتشاف ما وراء الإنترنت، بينها وبين نمط التعليم، أي بواقع عشرة متغيرات من أصل أثنى عشر متغيرا مدروسا.

تقارب وجهات النظر بالنسبة للرأي في أنظمة الحماية الأمنية التي يجب أن تتبع في مجال أمن المعلومات وأنماط التعليم المختلفة المدروسة لأصحاب العينة، بينما ثبت وجود علاقات إحصائية دالة بين ستة متغيرات فقط من جملة إحدى عشر متغيرا مما يثبت صحة هذا الفرض جزئيا.

تفوقت عينة نمط التعليم العسكري بالنسبة للرأي في مظاهر الاعتداءات على مواقع الإنترنت وعلاقته بنمط التعليم، وذلك في موضوعات القرصنة والهجمات النشطة، كالمعطيات والبرمجيات الوقتية والاعتيادية، والخدع، وجمع والتقاط كلمات المرور، والمسح، والنسخ، ويبدو أن هذه المظاهر تدخل ضمن مشروع أو مقرر تدريبي أو عملي يرتبط بنطاق تخصصاتهم أو وظائفهم أو دراستهم العسكرية، وبالتالي أنعكس على ترشيحاتهم لهذه المظاهر من الاعتداءات المختلفة على المواقع الإلكترونية المختلفة على الإنترنت والتي وردت في إجاباتهم من وجهة نظرهم، حيث أظهرت الاختبارات الإحصائية وجود علاقات دالة إحصائيا بين ستة عشر متغيرا من جملة 25 متغيرا مدروسا، وذلك عند مستوى دلالة (0.05) أو أقل مما يثبت صحة هذا الفرض جزئيا.

حدد المبحوثون أصحاب نمط التعليم العام العلماني، والأزهري، والعسكري من عينة الدراسة الهجمات النشطة في المستوى الأول كأهم المشكلات التي تقابل آليات الحماية الأمنية للمعلومات، ثم سلامة البيانات والاعتراض والاحتيال القانوني أو غير القانوني في الترتيب الثاني والثاني مكرر، بينما تفوق ذوي نمط التعليم الخاص في تحديد اختطاف القناة ومجال التشفير المحدود فبقية المتغيرات بعد ذلك، في حين تساوت إجابات المبحوثين من ذوي نمط التعليم الأجنبي في اختيارات بدائل الإجابات المختلفة على هذا السؤال بواقع اختيار واحد لكل متغير، في حين أظهرت الاختبارات الإحصائية وجود علاقات إحصائية دالة بين ستة متغيرات فقط من جملة عشر متغيرات، الأمر الذي يدعونا أن نقبل صحة هذا الفرض جزئيا.

34- كانت التحديات التربوية الداخلية هي أهم إجابات المبحوثين بالنسبة لذوي نمط التعليم العام والعلماني ويبدو أن هذين النمطين من التعليم يواجهان مشكلات داخلية على مستوى الطلبة والأكاديميين وعينة النخبة المبحوثة يجب أن يتم تداركها وإيجاد حلول لها، بينما جاءت التحديات الاقتصادية العالمية على رأس المشكلات العالمية التي يعاني منها ذوي نمط التعليم الأزهري، وربما يرجع ذلك إلى أن الميزانيات الداخلية قليلة وغير متعادلة مع أنماط التعليم الأخرى، أما بالنسبة لنمط التعليم الأجنبي والخاص فقط كانت التحديات العالمية بصفة عامة هي التي يعاني منها أصحاب نمط التعليم في هذه الفئة، وربما يرجع ذلك لارتباطها بتوجهات السياسة العامة العالمية والاقتصادية، والسياسية والتكنولوجية والتعليمية والأمنية وغيرها.

وجدت علاقة إحصائية دالة بين نمط التعليم وأشكال التهديدات التي يمكن أن تواجه الأمن المعلوماتي، تفيد ارتفاع رأى ذوي نمط التعليم العام والأزهري بالنسبة للرأي بالتهديد بتدمير البيانات، وارتفاع نمط التعليم الأجنبي والعسكري بالنسبة للرأي في التهديد بانتقاء المعلومات والتهديد باستغلالها وتساوي الآمر بالنسبة لنمط التعليم الخاص في كل المتغيرات المهددة بشكل عام.

رؤية مستقبلية واستشراف الاتجاهات الحديثة في مجال أمن المعلومات

إن الحاجة ماسة لوجود رقابة على المواقع الإلكترونية بصورة لا تتقاطع مع الحرية للحد من استخدامها لأغراض سلبية ويكون ذلك عن طريق سن قوانين الجرائم المعلوماتية وإعداد برامج تهدف لدخول المجتمع المعلوماتي تنتهجها الدول من أجل تحقيق الآتي:

1- الدفاع عن مصالح المجتمع وحقوق الأفراد أثناء استخدام تكنولوجيا تخزين ونقل المعلومات.

2- حماية موارد المعلومات المتوفرة في الشبكات المعلوماتية وتوسيع إمكانيات استخدام تكنولوجيا الإعلام والاتصال في كافة المجالات العلمية والتطبيقية للاقتصاد الوطني.

3- تشجيع وتعميم استخدام تكنولوجيا الإعلام والاتصال وتعميم أساليب المعلوماتية الحديثة في الأجهزة الحكومية قبل غيرها بغية تأمين حقوق المواطنين في تبادل المعلومات والحصول عليها من تلك الأجهزة.

4- تحسين ظروف وصول وتداول المعلومات التكنولوجية والتقنية والبيئية والاقتصادية والعلمية وغيرها من الموارد المعلوماتية عبر شبكات الإعلام والاتصال.

5- تطوير البحوث العلمية والبحوث التمهيدية في مجال تطوير تكنولوجيا وتقنيات الإعلام والاتصال.

6- ضرورة إن يمتلك قاضي النشر والإعلام خلفية عن الوسائل الافتراضية والإنترنت من أجل النظر في الدعاوي المعروضة أمامه في هذا الشأن.

7- يتم وضع كلمة سر على جهاز الحاسب الشخصي للولوج إلى الملفات المهمة أو حتى للنظام كله.

8- وضع برنامج أو أكثر من برنامج لمقاومة الفيروسات الإلكترونية الضارة، ويتم مراعاة الإجراءات الخاصة بحماية الدخول إلى شبكة الإنترنت والتأكد من مصدر البريد الإلكتروني.

9- يضاف للنظام جدران نارية تحد من دخول أشخاص من الخارج، وتمنع الاعتداءات المنظمة التي قد يتعرض لها النظام أو الموقع المعلوماتي.

10- إذا كان النظام يتبادل رسائل إلكترونية يخشى على بياناتها من الإفشاء، يكون التشفير مطلوبا بالقدر المناسب.

11- لابد أن تنطلق إجراءات الحماية من احتياجات الحماية الملائمة، لأنها إذا زادت عن حدها أصبحت ذات اثر سلبي على الأداء. إذا يصبح النظام بطيئا أو غير فاعل في أداء مهامه الطبيعية، كما أن نقص هذه الإجراءات عن الحد المطلوب يزيد نقاط الضعف، ويصبح النظام أكثر عرضة للاختراق الداخلي والخارجي كما تؤكد نتائج دراسات سابقة[17].

12- يجب أن تتضمن المناهج الدراسية المدرسية والجامعية مقررات في مجال أمن المعلومات.

13- لا يجب أن يكون هناك حرجا من الإفصاح عن أي اختراقات للأنظمة المعلوماتية وخاصة بالنسبة للمؤسسات المالية والاقتصادية، حتى لا ينتج عن ذلك خسائر كبيرة يصعب تداركها فيما بعد[18].

14- ضرورة الاهتمام بكافة أنواع الأمن المعلوماتي المادي والمنطقي وتطبيق كافة الخطوات الضروري في كل المراحل، مع ضرورة عمل خطط للطوارئ واختبار تلك الخطط في الظروف الاعتيادية.

المراجع

[1] Inman, A. James & Inman, R. Ralph Spring, 2006. "Responsibility as an Issue in Internet Communication: Reading Flames as Defamation", Journal of Technology Law & Policy, Vol. 11, No. 35, Available at: (http:Journal Law. Utl.edu, Techlaw/11/Inman. Html).

[2] داعوس، طلال محمد (2000). "العرب والعولمة: الظاهرة والتحديات"، الرياض، مجلة الدراسات الدبلوماسية، العدد 1420/14، ص175-184.

[3] Whitfield Diffie and Susan Landau, 2007. The Export of Cryptography in the 20th and In Karl de Leeuw, Jan the 21st Centuries Bergstra, ed. The history of information security, A comprehensive handbook. 725. Elsevier, p

[4] Boyd, D & Ellison, N.B., 2008. Social network sites: definition, history, and scholarship, Journal of Computer-Mediated Communication, Vol 13, No 1.

[5] Gurpreet S. Dhillon, 2002. Social Responsibility in the Information Age: Issues and Controversies, Published in the United States of America by idea Group Publishing,

[6] Aycock, J. and J. Sullins, 2010. "Ethical Proactive Threat Research," Workshop on Ethics in Computer Security Research (LNCS 6054), New York: Spring, PP. 231-239.

[7] زيدان، محمود، 2007. "نظرية المعرفة عند مفكري الإسلام وفلاسفة الغرب المعاصرين"، دار النهضة العربية للطباعة والنشر، بيروت، ص18-19.

[8] عبد الحميد، محمد، 2004، البحث العلمي في الدراسات الإعلامية، ص158-1589.

[9] المرجع السابق، ص158-1589.

[10] تم الرجوع في هذا التقسيم إلى: حامد، عباس رؤوف، 2006، الجامعات المصرية، ماضيها، حاضرها، مستقبلها، دار الشروق، ص12-14. http://ar.wikipedia.org/wiki/%D8%A7%D9%84%D8%A.

[11] we refered in this division due the following:

- Charles Doyle, (October 9, 2012)." Privacy: An Overview of the Electronic Communications Privacy" Act, Congressional Research Service 7.
- Bartell, C. 2011. "Resolving the gamer's dilemma," Ethics and Information Technology, 14 (1): 11-16.
- Bynum, T., 2000, "Ethics and the Information Revolution," Ethics in the Age of Information Technology, pp. 32-55, Linkoping, Sweden: Center for Applied Ethics at Linköping University.
- Scarfone, Karen, Souppaya, Murugiah, & Orebaugh Angela, (September 2008), "Technical Guide to Information Security Testing and Assessment", Recommendations of the national Institute of Standards and Technology, Special Publication, P.115.
- The Stealtrh Parody, friedrich Nietzsche, Available at: http://tvtropes.org/pmwiki/pmwiki.php/Main/StealthParody.

[12] we refered in this division due the following:

- Scarfone, Karen, Souppaya Murugiah, & Orebaugh Angela, (September 2008), Op Cit, P. 117. Retrieved: October 6, 2012.
- http://en.wikipedia.org/wiki/Covert_channel.
- Katantamalundu, D, Susan, (June, 2004), DEVELOPING A CRIME ANALYSIS FOR A INFORMATION SYSTEM POLICE SERVICE IN DEVELOPPING COUNTRIES', PHD THESIS, Enschede University, The Netherlands pp. 1-93.

[13] Hoven & Weckert (2008), "Ethics and Information Technology", 7(3): 111-119: Retrieved: June 6, 2011. http://plato.stanfor.edu/entries/it-moral-values/
[14] we refered in this division due the following:
- McMahon, J. M. and Cohen, R. (2009), "Lost in cyberspace: ethical decision making in the online environment," Ethics and Information technology, 11(1): 1-17.
- (August 2011). "New Us State Andy Leck, Law Impacts Manufacturers Worldwide That Use Stolen or Misappropriated Information Technology", Retrieved: January 12, 2014. http://www.bakermckenzie.com/ALSingaporeUSStolenITAug11/
[15] Brumley, David & Boneh, Dan, (2009). "Remote Timing Attacks are Practical", Stanford University Publications PP. 67-81.
[16] أنظر: سميشي وداد، (2010)، مرجع سابق، ص178-179.
[17] www.kkmaq.gov.sa/detail.asp?innewsitemid=164260&intemplatekey=print.
[18] http://www.alarabiya.net/programs/2006/01/15/20304.html.